ARTICLE APPEARED ON PAGE A1

NEW YORK TIMES
29 December 1985

U.S. Agency Makes Vast Plan To Encode More Information

By DAVID BURNHAM

Special to The New York Times

WASHINGTON, Dec. 28 — The National Security Agency has initiated a five-year program to encode most of the millions of electronic messages sent each year by the Federal Government and defense contractors.

At present a relatively small number of such messages are routinely encoded, primarily by the Central Intelligence Agency and other Government bureaus involved with national security. The N.S.A.'s program would extend to civilian agencies like the Agriculture Department and the Internal Revenue Service.

The agency will also try to persuade major private businesses like grain dealers, banks and stockbrokers to purchase coding equipment to make it difficult for outsiders to understand their communications.

The principal impetus behind the program is the belief of Government security officials that the Soviet Union has an active electronic surveillance program directed against the United States.

"This effort could cost billions of dollars but is worth every penny of it," Walter G. Deeley, the agency's deputy director for communications security, said in a recent interview.

The primary role of the highly secretive N.S.A., the largest spy agency in the country, is to intercept the electronic messages of other nations and to protect the sensitive information of the United States.

Controversy Over Role

Although the agency's responsibilities have been mostly limited to national security matters, President Reagan last year ordered it to assume the lead role in protecting the messages of the civilian agencies of government as well.

His order has been challenged on various grounds by two committees of the House of Representatives and by a number of organizations including the General Accounting Office, the Institute of Electrical and Electronic Engineers and the American Civil Liberties Union. Concerned about the National Security Agency's growing role, House panels have approved legislation that would place responsibility for the computer security of nonmilitary agencies with the National Bureau of Standards, a branch of the Commerce Department, rather than the N.S.A.

Evidence of the seriousness of the threat to electronic communications is largely anecdotal or, for security reasons, classified.

But Mr. Reagan, in ordering the National Security Agency to extend its communications concern beyond intelligence matters, said, "The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements."

From Soviet facilities in Washington, Glen Cove, L.I., San Francisco and Lourdes, Cuba, and similar listening posts operating from a new class of ships, the National Security Agency reports that Soviet specialists are scooping up large amounts of useful information by systematically eavesdropping on the nation's telephone and data networks.

The surveillance threat is heightened because most of these messages are now transmitted at some point by satellites or microwave towers. The interception of messages in the air is far easier to accomplish and far harder to detect than the interception of messages sent by underground cable. Several years ago, for example, there was speculation within the National Security Council that the Soviet Government was able to conclude a highly advantageous grain deal because of information it had obtained by eavesdropping on American grain dealers.

Other Tampering Cited

But concern about tampering by narcotics dealers, industrial spies and casual computer "hackers" has also contributed to the belief of many experts that communications security measures must be improved.

Just recently, for example, Government investigators broke up a narcotics ring that was operating highly sophisticated equipment capable of allowing the leaders of the ring to eavesdrop on the law-enforcement agents who were trying to arrest them. "There are a lot of medium-sized countries that would have been proud to have the signals intelligence operation of this group," said Mr. Deeley, the N.S.A. official.

One indication of the growing corporate concern about electronic eavesdropping, he said, is that in the last few years the International Business Machines Corporation has designed and installed equipment and procedures to encode its sensitive information. There have been reports in communications trade magazines that such techniques are already widely used in the oil industry, although the companies will not comment on the practice.

Another indication of the possible threat is the astounding growth in the number and power of computers and the information they contain.

100,000 Government Computers

In 1983, for example, according to estimates of the General Services Administration, the Federal Government had a total of 22,000 computers. This year, the G.S.A. believes Government agencies are operating well over 100,000.

Another rough measure of the growth of all kinds of electronic messages is the capacity of modems, the modulator-demodulator devices used to connect computers to communications networks like the telephone system. The N.S.A., for example, cited estimates that all the modems purchased in 1972 could together transmit about 600,000 characters per second. In 1984, according to agency calculations, sufficient modems were purchased in the United States to transmit 220 million characters a second.

Projects in the Works

According to briefings by Mr. Deeley and his staff at the headquarters in Fort Meade, Md., the National Security Agency effort may cost the Government about $40 million over the next few years and will include these projects:

¶The Data Network Security Project, a long-term effort aimed at improving the protection offered information transmitted around the United States on various commercial data and telephone networks like those offered by American Telephone and Telegraph, MCI and GTE. It also will include joint research with industry on techniques to improve security on local networks, like the electronic systems used to link the offices of a company scattered around a single city.

¶Project Blacker, a secret Defense Department project aimed at modifying the worldwide communication networks of the military to enable them to transmit messages that have widely varying levels of sensitivity without fear of interception. Virtually all details about Project Blacker are classifed.

¶The Development Center for Embedded Communications Security Products, a project involving a team of security experts from the N.S.A. and 11 leading computer and communications companies including A.T.&T., GTE, I.B.M., RCA, Motorola and Xerox. It

Continue

first began operating about a year ago, with the purpose of developing relatively inexpensive and easy-to-use devices that will encode and decode the messages generated on personal computers, cellular telephones and other communication systems.

Encoder for Personal Computers

The first example of the kind of product the agency hopes the development center will produce in the next few years is a security device code-named Gillaroo that can be installed in personal computers. The initial model of Gillaroo, named for a kind of trout found in Ireland, will be made available to qualified vendors in 1986. The agency hopes the vendors will begin offering personal computers equipped with Gillaroo in 1987 at an additional cost of somewhat under $1,000. The exact price will depend on the demand.

Gillaroo is a standardized module designed to scramble and unscramble classified information transmitted from the personal computers used by government agencies and defense contractors. It could be installed in new personal computers before they are marketed or added to existing personal computers. With the module, and a "key" that gives each unit its distinct code, the data being sent from modified computer would be almost impossible to intercept.

The various N.S.A. projects to improve the security of computerized data parallel a separate agency drive announced last year to provide Federal officials with 500,000 telephones designed to make eavesdropping almost impossible.

Mr. Deeley said the National Security Agency itself would spend $40 million in the next few years conducting research on low-cost coding equipment for personal computers and improving security of the commercial networks.

Billions of Dollars

But he added that if the joint research projects were successful, the low-cost equipment would become an almost standard feature of many personal computers and computerized networks. "We estimate that the total cost of really buttoning up all important data will be significantly less than 5 percent of the cost of the communications budget of the period in question," he said. Mr. Deeley acknowleged, however, that such an expenditure could easily total several billion dollars over five years.

Under the currently planned security system, the production of the encoding modules would be undertaken by American manufacturers who have been qualified to handle secret military contracts. Although the modules are being designed to resist efforts by scientists of other countries to figure out how they work, the data encoding devices used by government agencies and military contractors will require guarding.

Because the National Security Agency will be directly involved in the design of the modules and, in some circumstances, the distribution of the "key" needed to make it function, the agency will have the technical ability to decipher the messages transmitted through the modules.

"It is technically possible for the Government to read such messages, but it would be insane for it to do so," Mr. Deeley said. "It would be an exraordinarily expensive undertaking and would require a massive increase in computer power."

The official added that another important safeguard was the continuous review of the agency activities by the Senate and House intelligence committees.